AU/ACSC/SMITH, FI/AY16

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

BUILDING AN ADAPTIVE CYBER STRATEGY

by

Zachary M. Smith, Major, USAF
Master of Science, Strategic Intelligence, National Intelligence University

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisors: Lt Col Daniel A. Connelly and Dr. Panayotis Yannakogeorgos

Maxwell Air Force Base, Alabama

June 2016

Disclaimer

Abstract

Due to the complexity of cyberspace and the diversity of threats that operate in the new domain, current US cyber strategy has not proven effective. This paper dissects the cyber threat landscape and how advanced threats operate in order to devise an effective, adaptive strategy for US cybersecurity. US cybersecurity strategy must be threat-focused and threat-aware with capabilities built to evolve as threats evolve. Threat agnostic strategy that simply builds better perimeter defenses around victim networks is only part of what is needed to combat threats. To fill the gaps in modern cybersecurity, this paper explores the diversity of threats in cyberspace and how they operate by reviewing unclassified reports on advanced threats and augmenting this data by conducting interviews with leading cybersecurity industry threat experts. In addition to research on cyber threats, a firm understanding of US policy and the interagency policy environment is needed to properly design a cyber strategy. Research into US law and national policy included interviews with leading cyber policy experts in the federal government and private sector. This paper fuses knowledge about cyber threats and US law and policy to develop a strategy that accounts for the problems that have plagued US cybersecurity. The result is a strategy built with a cost-effective, multi-layered methodology that targets and disrupts threats to disrupt adversaries to decrease their overall effectiveness exploiting targets, and does not just place additional demands for ever-increasing spending in cybersecurity. By building better defensive hygiene, disrupting threat infrastructure, and manipulating threat organizations, this strategy provides a framework for the US government to organize for and operating in the cyber domain.

BUILDING AN ADAPTIVE CYBER STRATEGY

"If he sends reinforcements everywhere, he will everywhere be weak." – Sun Tzu[1]

An effective DoD cyber strategy must be built on a firm understanding of the strategic context of the cyber environment, because thorough knowledge of the threat landscape and the challenges the US will face is crucial to implement a plan that can achieve realistic goals in this new domain. Cyberspace exists within the physical world, and consequently cyber policy is subordinate to national foreign and domestic policy. In order to devise an effective strategy for cyberspace, we must understand the threats we are working against and the complexities of operating within our laws and policy as we move towards achievable strategic goals for the nation. The threats faced in cyberspace are varied, and a robust approach beyond cybersecurity is needed to combat advanced threats. Even if a perfect strategy is formed to combat advanced threats in cyberspace, it must function in the reality of the interagency policy environment; understanding the cyber policy landscape is essential to implementation of cyber strategy. After a thorough understanding of the adversary and ourselves, an effective strategy can be designed that will provide flexibility and resiliency without completely reforming the US government and the Department of Defense.

For almost two decades, the strategy of the United States in cyberspace focused on securing America's networks, which presumes that secure networks are attainable. Although the cybersecurity industry may exceed US$70 billion and continue to grow to greater than US$155 billion by 2019,[2] the growth of US dependency on cyberspace has likely exceeded the growth in cybersecurity resources, and may continue to do so indefinitely. The focus of US strategy on cybersecurity is logical, but incomplete. The strategy of diverting an ever-increasing amount of resources toward cybersecurity alone to defend every network against every threat is not cost

effective, and must be redesigned. This new threat-focused strategy takes into account who threats are and how they operate in a complex domain to provide a flexible and efficient capability to protect US national security interests in cyberspace.

Disrupt Cyber Threats

- Increase Defensive Hygiene
- Exploit and Disrupt Adversary Infrastructure
- Manipulate Threat Organizations

Build Capabilities

- Interagency Cooperation/Coordination
- Private Sector Integration
- Tactical-level Agency Integration and Counter Threat Teams

Necessary Qualities of Cyber Strategy

- Be Flexible across Threats and Spectrum of Conflict
- Prioritize Threats, Missions, Information/Technology, and Capabilities
- Ensure Readiness

Political Considerations

- Cooperate with Allies
- Demonstrate Restraint, Manage Escalation
- Create Norms to Reduce Threat Ambiguity, Ensure Intent is More Easily Inferred
- Deny Safe Haven
- Create the Least Amount of Change to Existing Policy and the Interagency Process

UNDERSTANDING THE STRATEGIC CONTEXT OF CYBERPOWER AND THE ROLE OF THE DOD

"The Air Force should institutionalize 'cyber-mindedness' and organize innovatively to successfully build capability and capacity for operating in cyberspace" – Maj Gen Stephen Miller, Commandant, Air War College[3]

Numerous government functions and the American way of life are now dependent on the interconnectivity that cyberspace provides, and there is increasing concern that critical weaknesses in cybersecurity could be exploited by foreign actors seeking to do us harm. The creation of a military force to act in and through cyberspace was a critical step in providing a capability to act in this new warfighting domain. The role of the US military is to defend the nation against external threats, prevent war, and build capability to exert cyberpower. The complexity of the role of the DoD in cyber strategy is that there is a need for judicious use of military power in and through cyberspace to support national security objectives, but this must be balanced with a doctrine of restraint to prevent the US from becoming an aggressor in this domain when the US portion of cyberspace is not adequately secure.

The cyber domain is more than a new location for kinetic military action; from a purely military perspective, the ultimate purpose of the domain is to maximize the effectiveness of military forces through the ability to communicate and distribute information and make more efficient decisions. Cyberspace is the domain where understanding of the battlefield is both presented and disseminated. Cyber capabilities allow a shared cognition of the battlespace and increased effectiveness of military decision-making processes. Cyberspace enables greater efficiency of modern militaries, and cyber-enabled militaries are indeed highly effective with less industrial-age resources. It is difficult to dissect the efficiency we have gained into quantifiable data points, but it is easy to see from the cockpit of the joint strike fighter to the

modern military command center that cyberspace has invaded every corner of warfare. The military has made cost decisions based on the effectiveness level that the cyber domain has enabled that cannot easily be reverted if our cyber advantage were to be impacted by an adversary. For the military, the true nature of cyberwarfare lies in the efficiency it provides to other military forces, governments, or civilians. It is the art of manipulating the effectiveness and ability of forces, both friendly and enemy, to reach decisions or control processes utilizing cyberspace by disrupting or enabling their cyber-dependent capabilities.

Militaries that have successfully harnessed the cyber domain are lethally efficient, but as the military grew more efficient through cyberspace it became clear that the military would need to defend this advantage in warfare. The cyber domain allowed the dismantlement of the industrial age military that did not rely on automation to maximize the lethality of a single soldier, sailor, or airmen. The US quest for shared cognition of the battlefield enabled commanders at all levels the ability to understand complex military environments quickly and maximize the employment of individual weapons systems with less resources. But where does this leave us? The US military is now dependent on cyberspace, the degree to which is not fully understood by military commanders.

Ambiguity and complexity surround this domain. Terms like “cyberwar” and “cyberattack” abound, implying there is a difference between the cyber version of these terms and their more mundane traditional brethren. Generation of kinetic effects through the cyber domain is simply warfare through a cyber medium. Cyberwar is a fictional concept that need not confuse policymakers and strategists. If a war occurs in cyberspace, it occurs in all domains. Military power in cyberspace should be controlled much like all military power is controlled. It will be important to build robust capabilities in peace to be ready to use cyberpower, but the

inherently deceptive anonymity the domain provides should not be used to create an idea that offensive military force should be used as replacement for effective cyber strategy. Operational capability is needed to disrupt threats in cyberspace, but this may not be the principle mission of the bulk of DoD cyber forces. The primary mission of the military in any domain, including cyber, should be readiness to exert force if needed during crisis.

UNDERSTANDING THE ENEMY

"The vast majority of threats can be stopped through better defensive practices, but the most sophisticated threats require a more robust approach."– John Davis, VP, Palo Alto Networks and former Deputy Assistant Secretary of Defense for Cyber Policy (Acting)[4]

The threats present in cyberspace are as varied as threats in other domains, and a one-size-fits-all approach is not sufficient for cyber strategy; we must understand the diversity of threats and build a plan that takes this into account. Strategy should be built in a way that reduces risk to national security through both understanding and limiting the effectiveness of cyber threats. We must be sure threats are unable to significantly impact the most vital parts of cyberspace, contained or managed in ways we choose. Advanced threats are able to bypass even well-built cybersecurity practices, and strategy must dissect how threats operate to provide the best chance of deterring or disrupting threat activity that exceeds acceptable levels. Although the details of threat operations may seem complicated and technical, they matter, and will greatly affect strategy development. As John Davis stated above, the great majority of threats in cyberspace can be stopped through better cybersecurity, but there is a limit to the upper level of cybersecurity effectiveness against advanced threats without significant redesigns of government and commercial networks. This section will explore those advanced threat operations in order to understand the implications for national policy and cyber strategy from the way sophisticated threats operate.

Cyber threats are broken down into groups based on attribution and intent. What is very unique in cyberspace is the degree to which the lines between these groups become blurred, potentially creating ambiguity and volatility. Broadly defined, the cyber threat spectrum is composed of hacktivists, criminals, spies, terrorists, and militaries. Often one group will use

another group as cover for action, but the groups are the starting point to understanding the cyber threat landscape needed to design cyber strategy.

Hacktivists: Hacktivists, a term first used in 1996 by the Cult of the Dead Cow, manipulate cyberspace to achieve political goals and social change.[5] Hacktivism is an entry point between political activism and more nefarious criminal activity on the threat spectrum. Hacktivists penetrate networks, disrupt services, deface websites, and steal information for the purpose of civil disobedience.[6] Sometimes hacktivists are entirely criminals using political activism as a cover for a purely criminal intent. Other times hacking activity in some countries is a legitimate political movement that goes right up to the line of criminal activity without definitively crossing it. The most prolific and well known of these hacker groups is Anonymous. The Anonymous group has been linked to campaigns against ISIS, the Chinese government, the CIA, and the Ferguson Police Department.[7] Although the targets of hacktivism are loosely organized around some type of perceived social injustice, the targets are very diverse and often disrupt legitimate governance functions. The members of Anonymous are as diverse as their targets. There is no formal organization of the group, which is composed of self-proclaimed anarchists.[8] As such, hacktivist groups like Anonymous can be highly disruptive and indiscriminate in their targeting. They often resort to denial-of-service attacks that can disrupt government functions not necessarily directly affecting their intended target. Nations have dealt with hacktivism very differently depending on the nature of their government. Democracies have

tended to use criminal investigative tools against them where more authoritarian regimes consider these groups a threat to state security.

Criminals: Criminal threats make up the considerable bulk of threat activity in cyberspace and are focused on profiting through violating rule of law. Global cybercrime activity is estimated to cost between US$300 billion and US$1 trillion.[9] Cybercriminals often operate from areas that are more permissive of their activities. Cybercrime may not pose as significant a risk to national security as other cyber threats, but the scale of this economic impact is not insignificant. Based on the criminal threat, several nations formed the Budapest Convention in order to cooperate to protect global society from cybercrime. This convention seeks to normalize cybercrime laws and increase cooperation with enforcement among member states, providing definitions and working towards norms for crimes such as child pornography, computer fraud, and various types of hacking and disruption activities.[10] Many nations have not adopted the Budapest Convention, and their cybercrime laws and general corruption issues provide areas of the world that allow safe haven for cyber criminals. Even in areas where there are extensive cybercrime laws and enforcement mechanisms such as in the US, cybercrime continues to expand at a rate that exceeds law enforcement capacity. The cost of entry for this criminal activity is extremely low. Although some cybercriminals are exceptionally capable hackers, some have almost no skills at all and obtain, purchase, and trade stolen data from computers through vast Internet communities. This loosely organized cybercrime activity trades mostly stolen identities or the hacking exploits/malware used to conduct hacking activity. Many tools are very simple to use. The US has devoted considerable law enforcement effort to combating identity-theft-related crime.[11] It is likely this threat will continue to grow and occupy many of the resources of law enforcement for the foreseeable future.

Spies: Cyberspace provides a new medium for spies to operate through, but espionage is not a new concept to national strategy and foreign policy. Espionage is one of the oldest nation-state activities; it was given considerable attention in the classic military work Sun Tzu's *Art of War*. In terms of foreign policy and international norms, spy activity occurs between both friends and enemies, often referred to as the second oldest profession.[12] State espionage even appears prominently in the Old Testament of the Bible, with similar texts appearing in many other world religions. The story of Joshua's spies involved details on espionage tradecraft including covert communication, and it demonstrated intelligence and counterintelligence activity that dates back thousands of years. [13] Although no treaties exist that allow for espionage to be conducted, use of spies and spyhunters are an accepted, or at least expected, practice by every nation state, and cyberspace is no exception.[14] If spies are caught, they are dealt with according to applicable domestic laws. In human intelligence, spies must risk their own safety by penetrating the target and could be prosecuted or killed based on the laws of the country they operate in. Cyber espionage has significantly less risk, requires minimal complicated operating locations in foreign countries, and is still easily accessible for less developed nations like North Korea.

Cyber espionage threats pose a significant risk to national security, but espionage is not the same as other types of nation-state activity in cyberspace such as cyberwarfare. Understanding the full extent of adversary intelligence activity cannot be known, and the blending of nation-state intelligence and military forces has greatly increased ambiguity and uncertainty while trying to determine adversary intent. The vast majority of nation-state activity in cyberspace likely falls under espionage and not warfare.[15] Many nations, like the US, operate with a close relationship between the National Security Agency and US Cyber Command. When a nation identifies activity from the anonymized infrastructure of an espionage organization like

NSA, it could mistakenly attribute the activity to US Cyber Command, a warfighting organization. Unlike preparation for cyberwarfare, espionage activity is not inherently escalatory. Cyber methodology employed for espionage purposes would generally be covered under criminal legal code; it may violate the domestic law of the targeted nation but does not violate international law.[16] Espionage activity does not constitute a use of force and is not considered warfare, but the prevalence of these threats still pose a significant challenge for cyber strategy.

Terrorists: Terrorism in cyberspace often receives a lot of attention, but terrorist organizations so far have not used cyberspace in the same manner as nation-state cyberwarfare. No terrorist organization has yet demonstrated the ability to cause widespread destruction or disruption through the cyber domain. Despite a low cost of entry in cyberspace, most organizations seem to lack the capability to cause military-like effects on their adversaries through the domain. Ideology is the foundational element of terrorism and cyberspace allows that ideology to reach across borders. The terrorist group known in the US media as the Islamic State of Iraq and Syria (ISIS) has proven to be very capable at using the Internet to further its objectives. According to Michael Steinbach, assistant director of the FBI's counterterrorism division, "the foreign terrorist now has direct access into the United States like never before."[17] The terrorist cyber threat presents a problem because of the maneuverability of information, violent ideology, through the cyber domain. However, many nations do not agree on what constitutes a terrorist. The Chinese, for example, label many dissident groups as terrorists that do not fit the same model as an organization like ISIS. Sometimes cyber terrorists present a problem for domestic law enforcement, and sometimes they are a threat for the military to confront. Because of this duality, a wide range of government organizations must work together to combat

terrorist threats in cyberspace, similar to the physical world. Terrorist threats in cyberspace can rise to national significance threatening regime stability, or operate as only a low-level domestic problem. They may be foreign or domestic based. As such, their makeup and methodology is widely varied and the threat they pose to national security reflects this variance.

Militaries: Although the use of cyberspace for military operations is not new, the use of cyberspace by the military to create offensive effects is a newer type of threat that is still very complicated to explore from a policy perspective. There is little consensus among nations regarding international norms about cyberwarfare outside of the already accepted Law of Armed Conflict (LOAC). Many nations see cyberwarfare as a new way to coerce adversaries. Cyberwarfare allows nations with a military disadvantage to compete against more powerful ones. The term cyberwar is often used to refer to nation-state conflict in the cyber domain, but there is no legal basis for this concept. War is a situation governed by LOAC. Terms like airwar and groundwar can be used to describe the portion of political conflict occurring in their respective domains, but they do not imply that there is a distinctly different legal structure governing each. The same is true for cyberspace. Labeling a chain of incidents as a cyberwar is only useful in the context of the greater political situation between the competitors. Cyberwar is not a useful independent concept because it implies conflict can be contained within the cyber domain. As Gen Michael Hayden states, it is often best to avoid the term altogether.[18] Warfare can indeed occur within cyberspace, but the effects are necessarily linked to other domains. Cyberwarfare is effects in cyberspace executed by nation-states.

Threats that execute cyberwarfare are the most potentially destructive of the threats in cyberspace. Military cyber threats have only recently risen to pose a serious concern for national security. Nations, including the United States, have invested heavily in preparation to fight in the

cyber domain. The tactics of cyberwarfare are still in their infancy, but the impact could be serious. It should not, however, be confused with cyber espionage. Espionage organizations may indeed conduct cyberwarfare, but this concept leads to increased ambiguity in the same way that warfare organizations often conduct espionage. Regardless, this highly ambiguous and complex threat spectrum requires a highly adaptive, innovative approach to have the maneuverability to transition authority across the threat spectrum without escalating the risk from the situation by adding to the ambiguous nature of cyberwarfare.

Understanding Threat Methodology: The blending of threat methodology and organizations has led to much confusion designing cybersecurity strategy. The United States has certainly contributed to this confusion by fusing an intelligence agency and a military warfighting organization. Although there were numerous advantages of this fusion that were needed when USCYBERCOM was created, it may be time to rethink how this affects perceptions in the cyber domain. Although nation-state threats are often military units, their activities have remained almost exclusively focused so far on either internal dissident control activity or foreign espionage. China is an example of such a country. What this means for cyber strategy is the dichotomy of how combat and espionage units conduct cyber operations must be taken into account. Agencies must necessarily cooperate to be effective, but that cooperation and blending of espionage methodology and infrastructure to conduct cyberwarfare is prone to lead to unnecessary escalation. There is a conception that an inability to attribute cyber actors nullifies escalation concerns, but a series of reports from Kapersky, Mandiant, Dell, Microsoft, Crowdstrike and many others demonstrates attribution may not be as difficult a problem, even for the private sector, as it once was.[19] Cyberspace threats do not readily present themselves in clean buckets with apparent methodology to link to adversary intent.

Threat Infrastructure in Cyberspace: The significant problem of determining intent and attribution of threats in cyberspace is caused by the similarity in the methodology all sophisticated threats use to deceive and penetrate targets and preserve anonymity. There is a wide range of techniques threats use to take advantage of flaws in cybersecurity, with names like buffer overflows, iframe redirects, and spearphishing, but the techniques are often dependent on building hacking infrastructure. The most sophisticated threats seek to avoid attribution, and this requires obfuscation of their point of origin. The two most common ways to obfuscate the origin of an attack is to either creating hacking infrastructure or use an airgap jumping capability. As an example of an airgap jumping attack, both Flame and Stuxnet used USB drives to spread the virus from one computer to another until they reached their intended targets.[20] Even if a threat uses this methodology as a vector, it is likely they will still build hacking infrastructure to enable some type of remote access to the target while maintaining the ability to mask the actor responsible, otherwise they have direct access to the victim network, and this is considered a traditional human infiltration of an organization.

The term "infrastructure" is used to describe many very different things in the cyber domain; hacking infrastructure describes the pathways adversaries use to conduct hacking activity. If the Internet is the "Information Superhighway" then hacking infrastructure is the pieces of that highway that hackers have to put together in order to create successful network penetrations. Dictionary.com defines "infrastructure" as "the basic, underlying framework or features of a system or organization; the fundamental facilities and systems serving a country, city, or area, as transportation and communication systems, power plants, and schools; or the military installations of a country."[21] Not to be confused with "critical infrastructure" that has a completely different meaning, the term fits well to describe the paths and necessary pieces

threats must build to support their hacking activity, and the term is widely used in cybersecurity. Each piece of hacking infrastructure serves a different purpose and all these parts have cybersecurity slang to describe them; they all form critical links in the way that hackers execute their activities. Infrastructure is primarily organized into three buckets: infrastructure owned by the threat, infrastructure compromised by the threat, and infrastructure leased by the threat. There is a physical component to hacking infrastructure; it exists somewhere in the physical world and is owned by an entity, either public or private. All computers and networks on the internet have ownership, the owner/operator pays the connectivity charges to the Internet Service Provider (ISP). Hacking infrastructure is almost always a necessary part of threat activity, and for nation-states the location of the infrastructure can greatly affect the legal and policy structures used for dealing with threats.

To obfuscate the hacker's point of origin, a hacker builds or purchases infrastructure to put a chain of computers between the source and the target. The source infrastructure is the computer or network that is usually owned/operated by the hacker. Very rarely do sophisticated threats directly access victims from computers on the source network, usually only by mistake. The intermediary group of computers in between are commonly referred to as "hop points" that relay commands between the source infrastructure and the target. Depending on methodology, these are sometimes called bots or zombies as well. Depending on the threat, these hop points can completely frustrate network defenses. According to Mandiant, the APT1 espionage threat operated nearly 1000 distinct and different hop points.[22] It is likely the number of hop points was much greater. Tracking threats almost never uncovers the totality of hacking infrastructure. Each piece of hacking infrastructure is used for a specific purpose in hacking activity. Some infrastructure functions as simple relays that do nothing more than pass commands from one

piece of infrastructure to another. Basic infrastructure purposes include command and control, relays, spearphishing, exfiltration, beaconing, webhosting, and more. Each of these pieces of infrastructure are critical links to how a hacker exploits a target, but they are often disposable if they are blocked at the victim. The primary purpose of infrastructure is to defeat the victim's attempts to easily identify hostile activity. Sophisticated threats often use numerous different hacking infrastructure locations to compromise a single victim, often with failover redundancy if one location is neutralized, making perimeter blocking ineffective against these threats.[23] Nearly all threats exploit flaws and vulnerabilities in cybersecurity practices, but sophisticated threats utilize robust hacking infrastructure and tools to enable and obfuscate their activities, and this methodology complicates the ability of governments to track, monitor, and attribute threats in cyberspace.

UNDERSTANDING OURSELVES

"But few of us (myself included) have created the broad structural framework within which to comfortably and confidently place these varied phenomena. And that matters. I have sat in *very* small group meetings in Washington, been briefed on an operational need and an operational solution, and been unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of *any* decision we might make." –Michael Hayden, former Director of the CIA, NSA, and Deputy DNI[24]

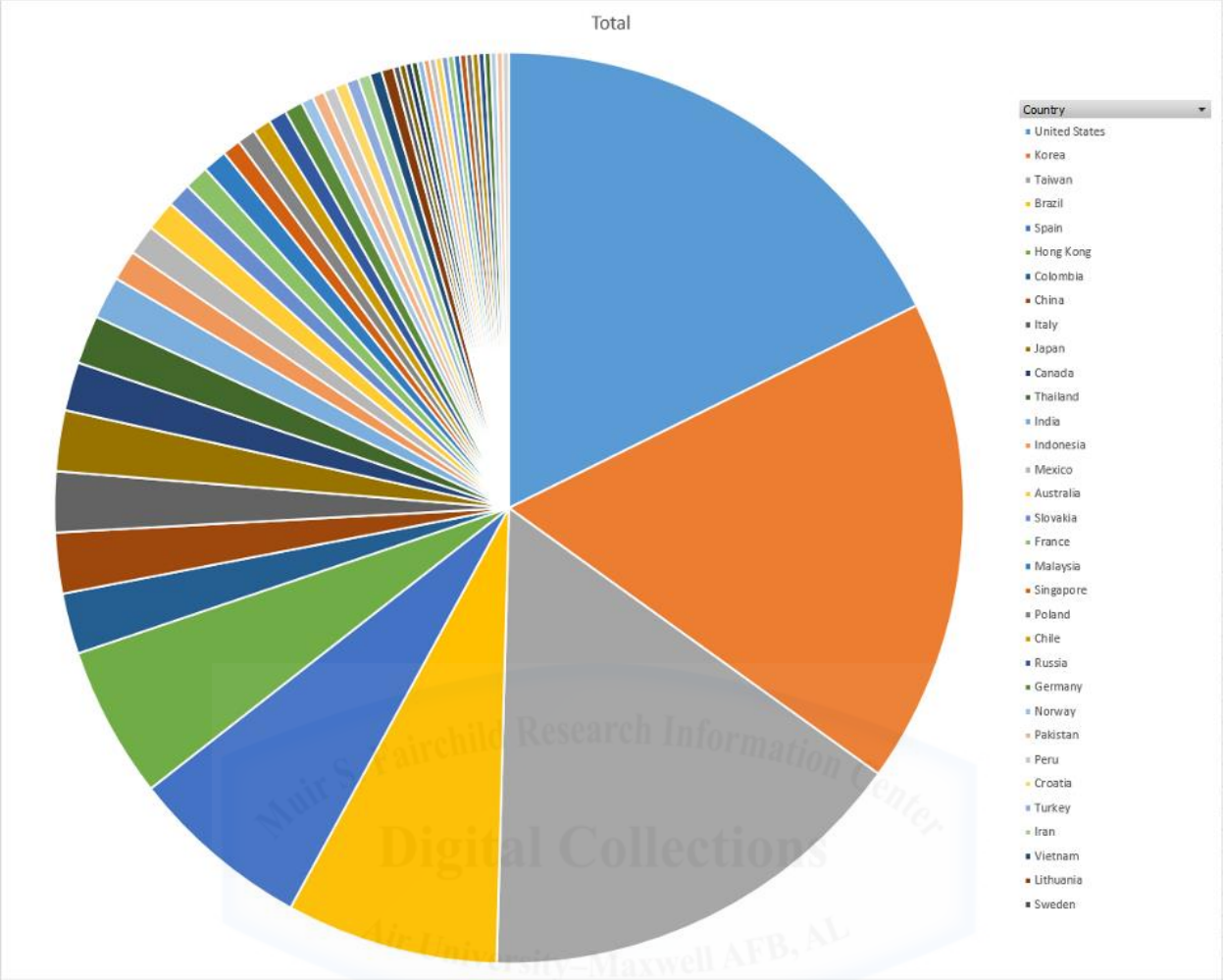
The blending of methodology by cyber threats creates difficulties in attribution, and this can lead to numerous problems designing cyber strategy. Consequently, cybersecurity, building better defenses, appears to be the defining principle in national cyber strategy. In 2003 the White House titled the national cyber strategy with the idea of securing cyberspace as the primary focus.[25] The White House shortened "cyberspace security" to cybersecurity and this vague term that implies a protected and secure end state now underpins many US organizations. The problem with cybersecurity is not the need to focus national attention to hardening and defending America's networks, but the idea that it is possible to actually achieve. The concept underpins all national strategy, but the investment is incredibly high to protect so large a construct from penetration from such a wide range of cyber threats. Sophisticated actors adapt to defenses in a way that makes a single flaw in cybersecurity sufficient for an adversary to exploit. With so much focus on cybersecurity, it leads to the perception that operational action is not a critical component of cyber strategy, but no security will ever be perfect, and operational action that can navigate the cyber threat spectrum is essential to ensure effective defense for critical missions.

The operational cyber policy environment is a complicated web of overlapping interagency authorities and capabilities, replete with role confusion. Coupled with many policymakers confused about the complexity of operations within the domain, it is a recipe for a disorganized strategy with overlapping political considerations further clouding effective

planning. The term “rice bowls” has dominated discussions about many different types of operations, and cyberspace is no different. As cyberspace emerged as nationally relevant, many organizations seem to have found this an opportunity for new funding lines, authorities, and political influence. Cyber policy is still in a state of flux and will continue to be so well into the future.

Physical geography is the most complicated obstacle for designing effective ways to counter cyber threats. Threats easily transition through cyber terrain distributed throughout the world by widely distributing their attack platforms. Meanwhile, US law and policy adds considerations for the geography of where cyber infrastructure actually resides in physical space. This has led many to lament the limitations that cyber policy places on operational action. The existing model of operational organizations may not be ideally suited to navigate the cyber terrain. Instead of focusing on reinventing operational authorities and procedures, it is important to fully understand the already existing ones and determine what relevancy this has in the cyber domain.

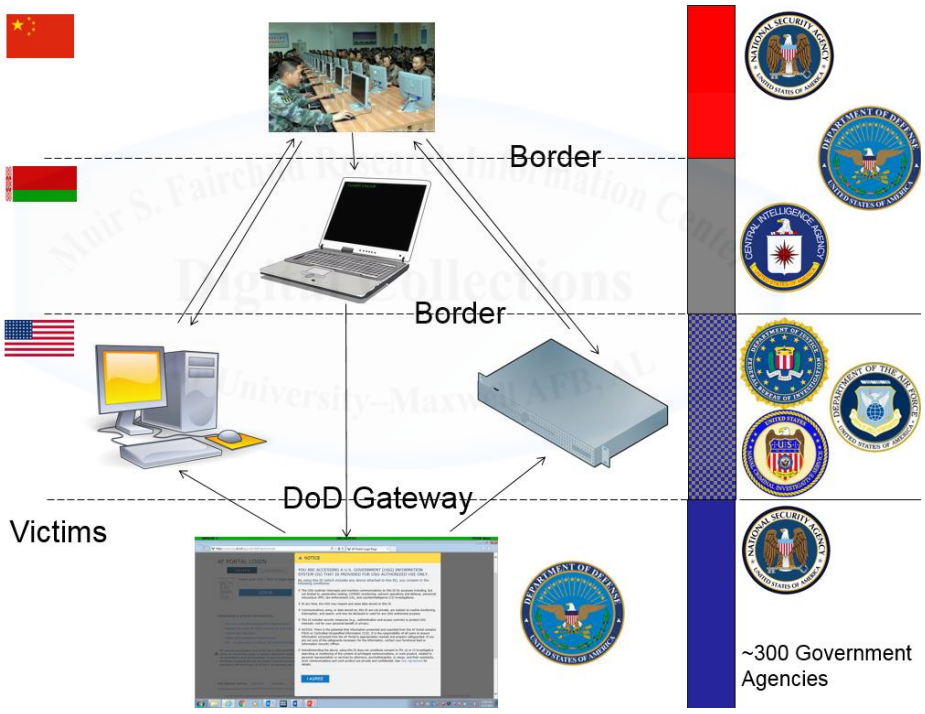
Hacking infrastructure is coopted, purchased, or leased by a hacker to conduct operational activity, and the dynamics of the infrastructure greatly affects the ability of defenders and operators to maneuver in cyberspace. Even if facing a military threat, the US military cannot easily maneuver to counter adversary actions through computers leased in the Amazon cloud or a hijacked point-of-sale computer from a local gas station, yet these all make up adversary hacking infrastructure and must be considered in strategy. As a very applicable example of threat complexity, a leading cyber threat expert from a Fortune 50 company has tracked the command and control hacking infrastructure of a single sophisticated threat; this threat has hundreds of hop points distributed across over 30 countries.[26]



The above chart shows the actual hacking infrastructure of an espionage threat from Asia, well known to the US government. The threat is most interested in victims in the US, Taiwan, and South Korea. What is most notable is that slightly over 50% of the hacking infrastructure for this state sponsored threat is within countries (US, Taiwan, and South Korea) that are the most likely targets for this group's espionage activities. The implications of where hacking infrastructure is located will have a significant impact on our ability to act against cyber threats.

A significant amount of policy discussion about cyber operations has focused on geography, a concept that is deliberately exploited by threats as seen in the above chart. US and international law and the policy governing operations have certainly placed important

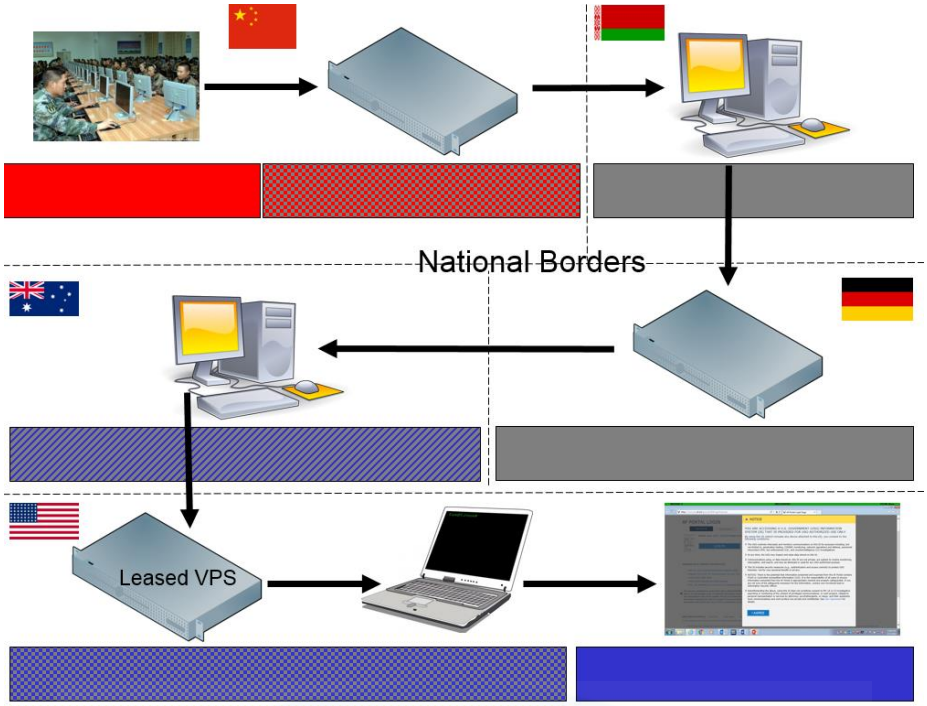
considerations for the geography of where cyber operations occur. Maneuverability in cyberspace is complicated due to this US interagency policy environment. It is complicated, but not impossible to navigate. Many organizations have restrictions on where they can operate based on the law their authority is based on. There are two ways to handle this limitation: 1) change domestic privacy laws and/or grant new authorities, or 2) determine which agencies have the necessary authorities and form a cooperative construct that enables cyber maneuverability against threats and operational action. The below chart depicts operational authorities superimposed on a typical espionage threat's hacking infrastructure.



The above completely hypothetical example demonstrates the most common conception in the breakdown of authorities to track, monitor and act against threats in cyberspace. US foreign intelligence agencies are responsible for threats overseas and hybrid law enforcement/counterintelligence agencies track and monitor threats domestically. In reality, law enforcement/counterintelligence force conduct extensive operations overseas, but the primary

coordinating authority will change based on geography. However, foreign intelligence agencies like the CIA or NSA are heavily restricted from conducting domestic operations. Finally, when a threat attempts to compromise a victim, over 300 federal agencies are responsible for defending their own networks as service providers. Derived from the Foreign Intelligence Surveillance Act (FISA) and Executive Order (EO) 12333, the typical intelligence community model is functional and tends to drive decision making, but it contains an incomplete view of how threats truly operate and the authorities of US agencies. Even with this simplistic model, it is clearly necessary to have strong interagency cooperation to track and monitor threats due to the complexities of where cyberspace actually exists within national borders, but the above model is not sufficient to understand the full foreign policy implications of cyber threat activity.

Unfortunately the above model of threat activity is incomplete and assumes a very convenient and straightforward threat infrastructure model. Hacking infrastructure exists in what is commonly referred to as grayspace, the non-governmental part of cyberspace containing hacking infrastructure that is disassociated from the sovereign governments responsible for the territory where the infrastructure resides. Grayspace has numerous layers. Each carry significant political and operational considerations. The below graphic shows the hypothetical hacking infrastructure of a Chinese espionage threat that is attempting to obfuscate its hacking activity by utilizing a complicated grayspace hacking infrastructure model:



In this example derived from data provided by industry experts on APTs, a Chinese threat exits their covered source infrastructure and compromises or leases infrastructure from an unsuspecting Chinese private entity in red-grayspace. The relay then travels to Belarus and enters true grayspace. Belarus has no knowledge the activity is occurring, is not a member of the Budapest convention to cooperate in cyberspace and deny safe haven to cyber criminals, and lacks capacity to combat cyber threats. Belarus fits the common perception of grayspace and is a nation on the far end of political grayspace foreign policy considerations. The hacking infrastructure chain then moves to Germany, where the US has numerous foreign policy agreements. There will be significant political considerations for any operational action taken in this country. Although Germany may be willing to cooperate in cyberspace, its own domestic privacy laws may complicate its speed of action, or prevent it altogether. The next link in the chain enters Australia by compromising a computer to build more hacking infrastructure. Australia has a robust capability to act against cyber threats, will freely cooperate with US

agencies, and their authority model closely matches the United States. Australian domestic intelligence agencies act within their sovereign borders. From there, the Chinese threat enters the US, appearing to come from Australia, and ends the foreign component of the hacking infrastructure. The complications of foreign policy will impact every link in the chain of this hacking infrastructure and will dictate what actions can be taken to monitor or disrupt this threat in cyberspace.

The last leg of grayspace will take the threat to servers in the US. As stated previously, the large majority of hacking infrastructure of a threat targeting the US is physically within our own borders, and US laws govern how agencies can act in this portion of grayspace. Contrary to popular reporting in the media, foreign intelligence agencies like the NSA and CIA are severely limited by US law and policy domestically.[27] Additionally, it seems since Edward Snowden there are many polls indicating there is little appetite in the American public for broader authorities for the NSA.[28] Due to extremely close ties with USCYBERCOM, this sentiment is often transferred to the cyber warfighting organization with regards to operations in domestic space where military action is often significantly complicated without the added intelligence and privacy complications. Only a very small number of law enforcement/counterintelligence agencies can operate in domestic grayspace. Still, domestic grayspace is critical to forming an effective cyber strategy since threats appear to consider the US an ideal area to build hacking infrastructure, and they exploit this area to maximize their ability to penetrate US targets.

A recent phenomena in threat activity is purchasing or leasing virtual hacking infrastructure, which presents new challenges for government action, but significantly exposes threats to the private sector cybersecurity community. This trend to move hacking infrastructure to the cloud, is exposing threats to a new community within the private sector that plays by very

different rules than the US Government. For instance, large organizations have no desire to have their brand associated with hacking activity such as "How Hackers Hid a Money Mining Botnet in the Clouds of Amazon and Others."[29] The private sector cybersecurity industry has adopted a different model than might be expected with regards to managing threat data. The cybersecurity industry is tracking and monitoring threats and is choosing to freely share threat data within a smaller, private cybersecurity community. In many cases they have formed binding agreements to cooperate to share threat data.[30] Most major cloud providers have terms of service that state illegal activity violates the lease agreements, and that they reserve the right to gather data related to the activity.[31] By leasing hacking infrastructure, threats are now exposing their operations while providing detailed financial data and covered identities that is ultimately traceable by corporations, perhaps more efficiently than the government. Interestingly, as service providers, the private sector can legally monitor and freely share data with each other relatively quickly, although they do not readily share or coordinate actions with the US government. Unlike the US government who tends to classify all data collected on hacking threats, the current trend in the private sector is to publish detailed reports attributing hacking groups, much like Mandiant and Crowdstrike have done. Groups that use leased hacking infrastructure may be exposed or disrupted by private sector cybersecurity groups that are much less restricted by US law or policy than the government itself. Leased infrastructure is still fairly new, and so it remains to be seen if this will end up being a safe haven for threats, or a unique vantage point for the private sector to act without government involvement to further collective cybersecurity. However, it will be difficult to predict how this dynamic will occur to incorporate it into national cyber strategy.

Understanding Authorities: Although cyberspace is still relatively new, threats operating in the United States are not new. Espionage activity has occurred in the United States

since the days of Benedict Arnold, and US law has taken this into account since its inception; it is the only crime in the US constitution.[32] The US government certainly has the ability to handle threats within its borders, so it is important to understand the implications of US agency authorities in cyberspace. Geography certainly has an impact on authority in terms of policy and procedures, but authorities are usually built around acting against threats while maintaining privacy. According to EO12333, the US foreign intelligence community identifies and reports on threats outside the borders of the United States.[33] Agencies like the CIA have special authorities to disrupt those threats in foreign countries. Each threat in cyberspace has an authority built in US code to counter it.

Criminal Investigative Authority: Law enforcement agencies are designed to deal with criminal hackers and hacktivism, which is a political extension of criminal hacking. Law enforcement is a broad authority that has a long history of use against state sponsored espionage threats and terrorists while operating within the constitutional requirements for operations within the United States. Domestic espionage investigations routinely end in criminal prosecution. The following press release from the FBI demonstrates just how applicable law enforcement is as a tool against the full range of state-sponsored cyber threats: “U.S. Charges Five Chinese Military

Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage."[34] That title shows how broadly law enforcement authority can be used to act against almost the entire cyber threat spectrum spanning criminal, espionage, and military cyber threats, but it is not intended to be the principle authority used in national security operations for monitoring and countering nation-state threats.

Counterintelligence Authority: Counterintelligence is closely related to law enforcement authority and is often one of the least understood authorities within the federal government. Broadly defined, counterintelligence is the authority created specifically to counter intelligence threats to the national security of the United States. The counterintelligence mission is defined in EO 12333 alongside the rest of the intelligence community of the United States.

> "Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities."

Counterintelligence is an inherently defensive, action-based authority. Under US law and policy, it is intended to conduct both monitoring/gathering activities and to act against foreign intelligence and terrorist threats worldwide. Additionally, unlike the majority of the intelligence community, there are policies that describe the procedures for counterintelligence to conduct domestic operations against foreign threats. With a domestic ability, it is potentially the most intrusive power in the federal government and is carefully regulated with strict guidelines on to safeguard domestic privacy under the constitution and law like the Electronic Communications and Privacy Act.[35] There are very few agencies with a counterintelligence mission. The CIA is responsible for coordinating the foreign counterintelligence mission while the FBI coordinates the mission domestically. Because of the significant risk espionage poses to global military operations and the technology needed to preserve the combat capability of the nation, the DoD

possesses counterintelligence authority. The Secretary of Defense and US law entrusted only specific, law enforcement-like, agencies within the military services with the authority to conduct counterintelligence missions, and separated these agencies from the joint warfighting construct of military operations. The Air Force Office of Special Investigations (AFOSI) and the Navy Criminal Investigative Service are hybrid agencies with both law enforcement and counterintelligence (LECI) missions, modeled similarly to the FBI. As part of the DoD, they also support military warfighting missions and counterintelligence missions overseas as well. Army Military Intelligence (MI) has no law enforcement mission and consequently has a slightly different counterintelligence authority structure. The Defense Intelligence Agency, as a foreign intelligence agency, also has authority to support missions in foreign space much like the CIA. Counterintelligence is a separated authority from within the greater intelligence community, intended to disrupt or defeat espionage threats both domestically or overseas.

Military Authority: Military authority is designed to protect the nation against attack and fight the nation's wars. The problem in cyberspace is an attack is not always obvious. The classical use of the military has been to fight other militaries in some state of declared conflict. Many senior military leaders have challenged this dynamic claiming there is a de facto state of war in cyberspace which could justify military operations against the attackers.[36] War is a political status that the military operates in support of, and military force in cyberspace has rarely been overtly used by any nation, if at all. Title 10, the law that governs the use of the military does cover the role of the military in cyberspace:

> "The Secretary of Defense shall develop, prepare, and coordinate; make ready all armed forces for purposes of; and, when appropriately authorized to do so, conduct, a military cyber operation in response to malicious cyber activity carried out against the United States or a United States person by a foreign power (as such terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801))."[37]

This language directs the US military to prepare for conflict in cyberspace, but limits military action to the existing authority and approval structures already in place. The use of military force to stop threats carries with it foreign policy implications.

The most notable offensive actions in cyberspace like the Sony attack or Stuxnet attack on Iranian nuclear reactors were never acknowledged by a government, moving them potentially into what the US might call "covert action." Unless military activity is acknowledged, clandestine military effects could end up being considered covert action much like special operations activities. Covert action is defined in Title 50 USC:

> (e) "Covert action" defined as used in this subchapter, the term "covert action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include—
>
> (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
>
> (2) traditional diplomatic or military activities or routine support to such activities;
>
> (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
>
> (4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.[38]

Covert action is very useful in cyberspace, but it is a highly complex authority of the intelligence community used to affect political or military conditions outside the United States, not necessarily to disrupt threats. Much like in other domains, military force in cyberspace is used extensively in the war on terror,[39] but is used only in extreme cases against nation states as military force can be highly escalatory.

There is certainly a critical role for military operations in cyberspace. The military forms the far end of US foreign policy, but the use of military force carries with it significant political considerations that have limited its use in cyber operations. The most significant consideration is

the "Act of War" conundrum described by Charles Dunlap. Dunlap describes when the Law of Armed Conflict applies and national security action can be taken. The two predominant structures he describes is the military model intended to eliminate threats through the use of force, and the law enforcement model that uses force only as necessary until other structures can be brought to bear.[40] Policymakers have been deliberately unclear as to what threshold is necessary to authorize a military response, in cyberspace or otherwise. If the nation suffers what constitutes an armed attack in cyberspace, it is likely a military response will be directed. Although many in both the military and the private sector have adopted the term "attack" to describe any unwanted activity in cyberspace, the President has not publically authorized any military action by invoking the right of self-defense. Escalation has been a significant concern for policymakers and using military force to stop espionage activity appears to complicate matters. The final complication for the military in cyberspace is that military actions are highly limited within the United States under strict rules, and threat infrastructure is likely to continue to be built domestically.

The Interagency: Cyber threats have learned the seams in US agency authorities and exploit the inherent complications of interagency operations. US law and policy grants authority for some component of the federal government to act in all phases of conflict and against all threats. There is no authority that is lacking to disrupt threats in cyberspace. What continues to frustrate operational action is the complexity in gaining approvals and coordinating cyberspace operational activity. Still, the US has achieved some significant successes and developed some innovative approaches toward dealing with threats in the cyber domain despite traditional interagency rivalries.

THE DESIGN OF A VERSATILE CYBER STRATEGY

"He who defends everything defends nothing." – Frederick the Great[41]

The United States needs a flexible and adaptive strategy to defend against the full range of cyber threats based on the complexity of how those threats operate. The current national cybersecurity strategy has moved significantly forward, but is not sufficient to disrupt advanced threats in cyberspace. Since at least 2003, national strategy has focused on creating a secure cyberspace. The foundations of the current cybersecurity strategy are sound as a necessary baseline, but cybersecurity will always be imperfect, and capabilities are needed that can compensate for flaws in the system. Cyber defenses must have a more robust capability to defend critical information, operations, and control systems. Organization of cyber capabilities at both the strategic and tactical levels can no longer be organized in stovepipes; cyber forces must have maneuverability to operate across the threat spectrum as needed. Civilian organizations must become more than just victims to protect through information sharing or mitigation; they must now be integrated into operational activity to disrupt threats and incorporated into strategy. Finally, the DoD must evolve to meet the needs of national strategy. This recommendation for cyber strategy is not intended to be comprehensive, but serves as an overview of how the nation should be organized for effective defense of cyberspace.

The cyber domain has significantly changed since the creation of the Internet, and cyber strategy should not be a one-size-fits-all defensive approach. Since at least the 2003 national strategy, America has focused on raising the bar in cybersecurity. According to Internet Live Stats, there were approximately 415 million Internet users in 2000; in 2005 that number had reached over a billion; in 2016 it is estimated at over 3 billion users.[42] The chart below shows that nearly half of the world's population is now online.

Year	Internet Users**	Penetration (% of Pop)	World Population	Non-Users (Internetless)	1Y User Change	1Y User Change	World Pop. Change
2015*	**3,185,996,155**	43.40%	7,349,472,099	4,163,475,944	7.80%	229,610,586	1.15%
2014	**2,956,385,569**	40.70%	7,265,785,946	4,309,400,377	8.40%	227,957,462	1.17%
2013	**2,728,428,107**	38%	7,181,715,139	4,453,287,032	9.40%	233,691,859	1.19%
2012	**2,494,736,248**	35.10%	7,097,500,453	4,602,764,205	11.80%	262,778,889	1.20%
2011	**2,231,957,359**	31.80%	7,013,427,052	4,781,469,693	10.30%	208,754,385	1.21%
2010	**2,023,202,974**	29.20%	6,929,725,043	4,906,522,069	14.50%	256,799,160	1.22%
2009	**1,766,403,814**	25.80%	6,846,479,521	5,080,075,707	12.10%	191,336,294	1.22%
2008	**1,575,067,520**	23.30%	6,763,732,879	5,188,665,359	14.70%	201,840,532	1.23%
2007	**1,373,226,988**	20.60%	6,681,607,320	5,308,380,332	18.10%	210,310,170	1.23%
2006	**1,162,916,818**	17.60%	6,600,220,247	5,437,303,429	12.90%	132,815,529	1.24%
2005	**1,030,101,289**	15.80%	6,519,635,850	5,489,534,561	12.80%	116,773,518	1.24%
2004	**913,327,771**	14.20%	6,439,842,408	5,526,514,637	16.90%	131,891,788	1.24%
2003	**781,435,983**	12.30%	6,360,764,684	5,579,328,701	17.50%	116,370,969	1.25%
2002	**665,065,014**	10.60%	6,282,301,767	5,617,236,753	32.40%	162,772,769	1.26%
2001	**502,292,245**	8.10%	6,204,310,739	5,702,018,494	21.10%	87,497,288	1.27%
2000	**414,794,957**	6.80%	6,126,622,121	5,711,827,164	47.30%	133,257,305	1.28%

* Estimate for July 1, 2016
** Internet User = individual who can access the Internet at home, via any device type and connection.

The explosion of online availability means there is significantly more computers available in both the US and developing countries that can be compromised and exploited as a victim, or used for hacking infrastructure. Better global cybersecurity practices should increase the time advanced threats must spend to build hacking infrastructure, decreasing their overall efficiency. That means less time that threats can spend compromising actual targets, instead focusing more resources on building infrastructure, but this is a very long term goal.

Threat-Aware and Threat-Focused Cybersecurity: The cost of perfect cybersecurity has continued to grow at rates that are only rivaled by the rate that cyber threats have grown. In the words of Winston Churchill, "Gentlemen, we have run out of money; now we have to think."[43] We should endeavor to keep raising the bar and building better cybersecurity globally,

but we need to evolve to a national strategy that seeks to understand threats and adapt as threats evolve. We need to have redundancy to act at multiple levels, should one level of defense fail. We cannot just focus on building pristine cyber hygiene and expect advanced threats will not be successful at exploiting targets. There is a better way to defend against threats that understands the nature of the enemy and the nature of ourselves. The below table is a cyber strategy that can execute subordinate to the National Security Strategy of the United States to defend against threats in cyberspace.

Disrupt Cyber Threats
• Increase Defensive Hygiene • Exploit and Disrupt Adversary Infrastructure • Manipulate Threat Organizations
Build Capabilities
• Interagency Cooperation/Coordination • Private Sector Integration • Tactical-level Agency Integration and Counter Threat Teams

Disrupt Cyber Threats: The first premise of effective cyber strategy is that cybersecurity is only needed because threats in cyberspace exist; an effective cyber strategy must be threat-aware and threat-focused. A threat-based strategy allows agencies and the private sector to focus attention and resources where it is needed most to stop threats from being effective against their targets. This cyber strategy takes into account two factors: 1) who the threats are, and 2) how/where they operate. Threat management is at least as important as better defensive hygiene. There are three points where a threat can be disrupted. The first location is at the victim, but victim defenses are the most expensive part of cybersecurity funding. The

President's latest proposal will invest over $19 billion into cybersecurity. By 2020, there could be over 75 billion devices connected to the Internet.[44] Cybersecurity funding may grow with the explosion of devices, but building better defensive perimeters is far beyond the capability of the federal government to solve. Private industry must continue to build better platforms with less attack surface. The US way of life is heavily reliant on a secure cyberspace, but the complexities of interconnected, global networks make it impossible to fully defend everywhere against all threats. As adversaries grow more sophisticated, more resources are needed to build better defenses for more networks, with an advantage to the attacker. A more resilient and cost-effective strategy augments perimeter network defense with smart use of counter-threat operations.

Increase Defensive Hygiene: Defeating the most widespread and basic online threats demands industry best practices/standards and better cyber hygiene. Unsophisticated criminals have become too great a threat to the general public as more and more people move online with only limited knowledge of cybersecurity. The President's Cybersecurity National Action Plan (CNAP) states that the cyber domain has reshaped the way the American economy works.[45] The President's position to improve information sharing, modernize government networks, and cooperate with the private sector is essential as a baseline for cybersecurity.[46] The President extends this defensive strategy to private individuals by stating "empower Americans to secure their online accounts" in the national strategy. John Davis, former Deputy Assistant Secretary of Defense for Cyber Policy (Acting) and the Vice President of Palo Alto Networks states that the vast majority of threats can be defeated though better defensive practices.[47] Many other senior government and private sector officials would likely agree. This essential baseline is necessary to

reduce the amount of threats to a more manageable level so that major governmental action can be directed at the truly dangerous advanced threats in cyberspace.

The way both the private sector and government think about cyber defense needs to be retought based on the spectrum of threats. In "The Future of Things Cyber" Gen Hayden asks the question, "Is defense possible? Is the web so skewed toward advantage for the attacker that we are reaching the point of diminishing returns for defending a network at the perimeter (or even beyond) and should now concentrate on how we respond to and recover from inevitable penetrations?"[48] Defense is indeed possible, and likely highly effective, but not if treated as an all-or-nothing solution. The way we think about our perimeter has to change. Perimeter defense must not be our only line of defense. Nor should agencies focus incredible resources on building complicated defense in depth throughout their enterprise if it is not warranted. The most important step in defending a network is determining what *actually* needs to be defended, and from whom. For instance, a defense contractor working on the 5th generation fighter for the US Air Force has a much higher likelihood of being targeted by a nation-state threat and needs to have *a portion* of their network defended against the most advanced threat. The same applies to critical missions of the government. For a typical business, customer Personally Identifiable Information (PII) may be the most important target, but this most likely will be targeted by cyber criminals, not nation states. Intellectual property is often the lifeblood of many major corporations, potentially targeted by both criminals and nation states, and it should be guarded in a way much different than the company work schedule, based on what threat might be interested in taking it. Cybersecurity companies should offer this kind of service as part of cybersecurity packages, with analysis of the most likely threats to the target in mind. This will never be a

perfect solution, but if done in concert with the other parts of this strategy, it will be effective in reducing the capabilities of threats over time without as significant of cost.

Exploit and Disrupt Adversary Infrastructure: A baseline cybersecurity effort cannot stop advanced threats everywhere, all the time. The second part of the statement by John Davis, "…but advanced threats require a more robust approach" describes the need for both the government and private sector to work together to defeat sophisticated threats. Advanced threats may fall across the threat spectrum and exploit complicated hacking infrastructure, and so different agencies, working together will be responsible for threat pursuit operations depending on the specifics threat. The complexities of threat makeup and hacking infrastructure mixed with agency authority is nothing to fear in cyber strategy. It must be implemented in the least-escalatory manner possible, based on a doctrine of restraint. There is no possible way to ensure a completely secure cyber environment anytime in the near future. The diversity and complications of potential targets means there will inevitably be flaws somewhere in the system. Cyber operations must pursue and frustrate cyber threats wherever they go, including hacking infrastructure. Infrastructure operations must include a mix of public, private, and foreign government cooperation as well as direct action. A diverse presence is intended to increase the cost of doing business for advanced cyber adversaries. The objective of infrastructure operations should not be to stop threats, but disrupt them by taking clearly defensive, not offensive action. Hacking infrastructure is inherently disposable so choosing when, where, and how to engage is critical. To be successful in disrupting threats, the United States must accept the realities of how advanced threats build and use their hacking infrastructure.

Operations to disrupt adversary infrastructure include a range of options and defensive practices. The most basic option is blocking known hostile adversary infrastructure. This basic

defensive practice is routinely done without any regard to adversary behavior. Just knowing an adversary uses a piece of hacking infrastructure is not an adequate reason to block it. Information sharing is key to understanding what practices are most appropriate. For advanced threats, infrastructure may be the only indicator a defender has that hostile activity is occurring. Blocking advanced threat infrastructure is similar to stepping on ants one by one to cure an infestation. Blocking should have a coordinated purpose towards managing the threat. John Lambert at Microsoft describes a theory that takes into account both threats and network design.[49]

Lambert's theory about the differences between the modern defender and the traditional defender has utility for defenders, but the most notable part for strategy is the idea to manage adversaries, not incidents. Defensive actions must have purpose based on threat knowledge and not just follow a checklist. The best strategy may be to collectively drive advanced threats to a position of greatest advantage for defenders, and/or make threats less efficient. This strategy is broader than just technical actions. If Belarus is unwilling or unable to cooperate in cybersecurity, then effective defensive practices can support diplomatic efforts with that country by coordinating blocking actions more broadly as a part of overall strategy.

Last, a robust capability must be developed to disrupt the overall effectiveness of adversaries on their own hacking infrastructure. Threat agencies and the private sector should maximize their ability to act to disrupt the way threats operate. The focus of these actions should be to increase the cost of doing business for advanced threats over time, not to stop every attack, which is impossible. There are numerous examples of robust, cooperative counter-infrastructure operations. In April of 2015, Trend Micro, Interpol, Microsoft, Kaspersky, and the Cyber Crime Institute all collaborated to takedown the SIMBA botnet leading to a disruption of botnet activities.[50] The private sector is ideally suited to cause widespread disruption of hacking infrastructure with tools like the Microsoft Malicious Software Removal Tools or antivirus software from vendors like Symantec running on computers throughout the world. Once a specific tradecraft becomes widespread, it can be eliminated. The private sector is usually a neutral actor from a standpoint of policy. Corporations are willing to support government actions to disrupt threats, but are just as incentivized to stop their own governments from breaking into computers running their operating systems or antivirus. Some situations will require a more targeted solution from the government to disrupt threat effectiveness. Ultimately infrastructure operations can account for flaws in the defenses of victims and disrupt threats giving time for defenders to act.

Manipulate Threat Organizations: Although cyber threats are diverse, all are made up of people, and people are vulnerable to the instruments of policy. There is nothing unique about this fundamental part of an effective cybersecurity strategy, and it has been effectively employed repeatedly over the course of several administrations. For example, the previously mentioned indictments of 5 Chinese military hackers certainly attracted the attention of Chinese political leadership, and generated a storm of political repercussions.[51] Directly targeting a hacking

organization through law enforcement tools was toward the more aggressive end of escalation, but it likely achieved a disruption of Chinese-based cyber threat organizations. Disruption of threat organizations is not exclusive to the US government. The private sector has achieved similar successes. The now-famous Mandiant report resulted in widespread media coverage of the exact building the alleged Chinese espionage unit 61398 occupied, including a rather dramatic video of Chinese internal security chasing and detaining a CNN reporter.[52] The attention on this espionage unit generated by a private corporation effectively dissolved the anonymity needed for intelligence operations in cyberspace. Private sector capabilities to track and monitor threats continue to grow due to private information sharing agreements and sophisticated threats increasingly lease hacking infrastructure in the cloud instead of just compromising hop points. This has given the private sector new capabilities to manage and disrupt significant threats in cyberspace. Acting independent of government direction, private sector involvement is likely to be a more common way to disrupt threats in the future. The full range of public and private capabilities that should be employed to disrupt threat organizations is too many and varied to list, but they include numerous parts of the intelligence community, diplomatic, economic, and military capabilities of the United States. Even if the other two parts of this strategy are ineffective against a threat, targeting a threat organization can compensate for flaws in the system.

Build Capability to Disrupt Threats in Cyberspace: The existing construct of cyber strategy is focused on building better walls to keep the threats outside. Though all the pieces of effective cyber strategy exist in the government, they are not tasked or organized to maximize efficiency in cybersecurity. For instance, at this time, the preponderance of advanced cyber threats are hostile foreign intelligence. Because of threat ambiguity, those same intelligence

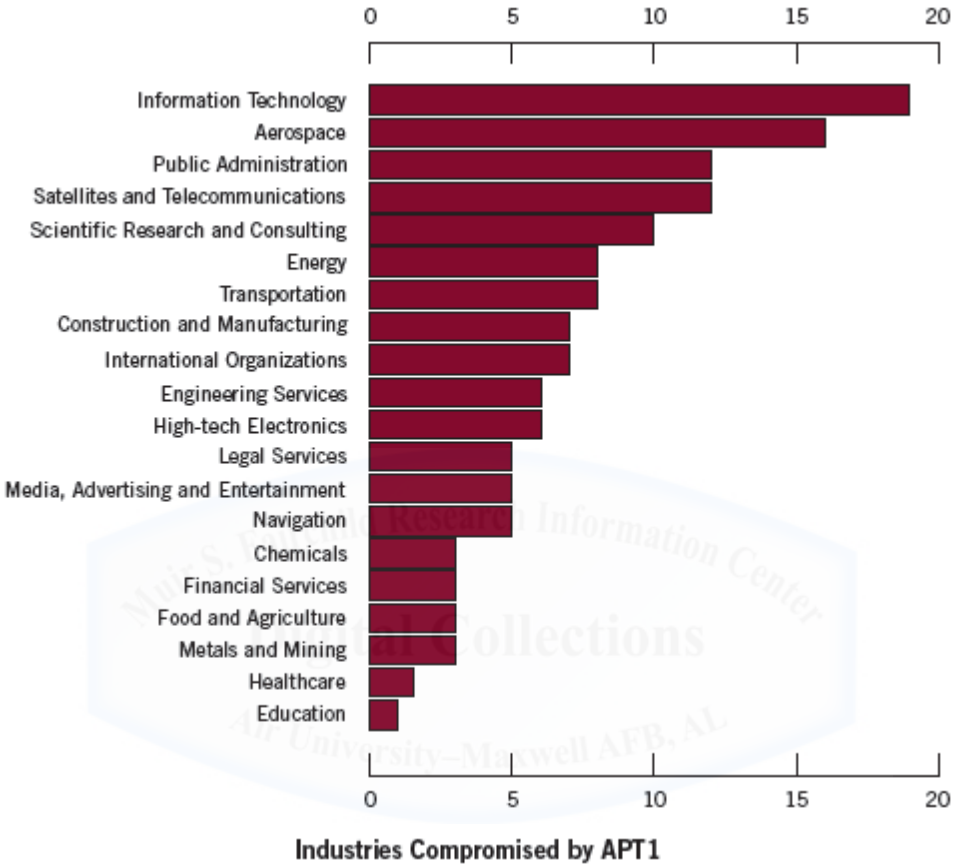
threats may transition to a military threat if relations with that country were to deteriorate. An industrial age mindset would build robust counterintelligence agencies in time of peace to fight the espionage threat, but that would also necessitate building robust military capabilities for time of war. The problem with threat disruption operations stems from capacity. Counterintelligence forces need more capacity in time of peace and military forces need more capacity in time of war. The FBI is primarily responsible for the conduct of domestic counterintelligence operations, but disruption of nation state intelligence is a mission shared by the FBI with DoD service counterintelligence agencies, and is currently not done by military warfighting organizations. Counterintelligence, including DoD counterintelligence, operates closely with law enforcement under similar processes to meet constitutional requirements. But the capacity is often augmented through a variety of support means to enable disruption of threats. Operational capability should be able to transition through the threat spectrum appropriately, while minimizing potential escalation of a situation through military effects operations against a non-destructive intelligence threat.

The mission to disrupt intelligence threats already exists within the DoJ and DoD and routinely conducts activity designed to disrupt espionage threats impacting national security. Though risk balance is a part of all operations, counterintelligence works within the thresholds of acceptable foreign policy and domestic law. All nations states conduct both intelligence and counterintelligence activity and the presence of this activity is usually not considered escalatory. The implementation of intelligence activity is often closely associated with diplomatic institutions like embassies, though rarely directly associated. The presence of intelligence forces within another sovereign area is expected, and often counterintelligence tracks, monitors, and disrupts these threats globally.[53] The construct of joint military warfighting is not built to handle

the intricacies of counterespionage or counteintelligence effects operations. The capacity of government threat disruption capability needs to be flexible enough to adapt to threat ambiguity while managing the risk of escalation. If a threat is espionage, threat disruption operations should be handled through counterintelligence agency processes, which are even authorized to conduct counter-sabotage operations if needed. But, if conflict occurs, military forces need to be prepared to act, and should be aware of counterintelligence operations in order to increase capacity when needed while remaining in a support role unless those threats transition to warfare activities. If the US builds both the capacity needed to disrupt espionage threats and military threats, it must double the capacity of the adversary who will transition between espionage and military operations as needed during peacetime of conflict. The capacity problem means many forces will conduct less activity depending on the spectrum of conflict, creating waste, and may not be prepared to act against adversaries if foreign relations change. A new construct is needed to ensure agencies work together to implement cyber strategy instead of adopting inflexible agency-specific industrial-age approaches that do not take into account threat ambiguity.

Interagency Cooperation/Coordination: Threats are well aware of the difficulties US agencies have tracking threats across hacking infrastructure. The private sector has proven it is both capable and willing to navigate the seams that US policy has struggled with. The problem has arisen because the role of US agencies is often clouded with regards to cyberspace. For instance, the mission to protect critical infrastructure has a shared role for DHS, FBI, DoD, and any number of sector specific agencies, and the private sector is often responsible for actually operating the target networks. Depending on the sector, each agency may have a more prominent role. This is often easily defined. All agencies share a part, but some have a greater vested interest. There are over 300 federal agencies that are responsible for supporting cybersecurity

efforts at a victim, but often when this moves to hacking infrastructure, threats overlap. A nation-state threat is unlikely to target only a single sector. In the case of APT1 from the Mandiant report, 20 industries were targeted by a single espionage threat.[54]



Industries Compromised by APT1

This is a recipe for interagency confusion, but it need not be. Protection against threats to Aerospace is as critically important to the DoD in defense of the nation as other sectors are to the FBI. Each agency was created because of the criticality of the mission they were designed and funded to accomplish. The government must adopt a shared, collaborative approach to operations and get rid of the idea of an exclusive best athlete approach or it will not be able to effectively disrupt threats. No single agency has all the capability or capacity needed to affect all cyberspace threats across the spectrum of conflict. There is considerable investment in well-established stovepipe organizational processes that may be in conflict with the innovative solutions needed

to disrupt threats. There is still little incentive for agencies to work together but the reality of cyber threat methodology requires cooperation to be effective.

Government agencies must work using their existing policy, procedures, and approvals, but a better task force construct is needed to measure the effectiveness of each organization in supporting interagency operations. The most ideal function would be to build an organization to oversee and implement the national cyber strategy. The National Security Council (NSC) cannot serve this function; the NSC does not direct agency action. The power of the NSC is to organize meetings.[55] Although there are numerous cyber task forces and interagency constructs, no such operational oversight organization currently exists. Last year the President created the Cyber Threat Intelligence Integration Center (CTIIC).

> "The CTIIC will be a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers. The CTIIC will also assist relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats."[56]

The CTIIC is an example of one part of an organization necessary for an effective counter-threat strategy. The CTIIC, in theory, fuses intelligence data from across the community to provide a common sight picture of the adversary, but it does not implement cyber strategy or direct/coordinate operational action. The National Cyber Investigative Joint Task Force (NCIJTF), which was created during the Bush Administration, includes most of the parts necessary, with the exception of the implementation of cyber strategy.

> As a unique multi-agency cyber center, the NCIJTF has the primary responsibility to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation.
> The NCIJTF also synchronizes joint efforts that focus on identifying, pursuing, and defeating the actual terrorists, spies, and criminals who seek to exploit our nation's systems. To accomplish this, the task force leverages the collective authorities and capabilities of its members and collaborates with international and private sector partners

> to bring all available resources to bear against domestic cyber threats and their perpetrators.[57]

FBI led and primarily domestic focused, although the principle Deputy Director is NSA, the NCIJTF is most effective as an information sharing or coordination capability for domestic investigations. It is closely aligned with the FBI mission, and serves a critical collaboration role in infrastructure and counter-threat operations; however, the NCIJTF is built on liaisons and does not fully leverage the full capability of the nation or the government to execute cyber strategy. In order to execute a full range threat-focused strategy, a national operations-focused organization is required for effective cyber strategy implementation that focuses interagency action without just incurring a tax on agencies for another liaison.

Private Sector Integration: The role of the private sector is critical to an effective cyber strategy, but this partnership with government must extend beyond information sharing to cover the entirety of counter-threat operations. As evidenced by detailed threat intelligence products like Mandiant's report on People's Liberation Army (PLA) Unit 61398[58] and Crowdstrike's report on PLA Unit 61486,[59] the private sector is effectively tracking and monitoring threats in cyberspace. Many major cyberspace-related corporations are willing to cooperate with the government to disrupt cyber threats, often out of patriotism.[60] Other private sector entities simply see positive financial benefit to cooperation in cybersecurity. Fortinet, Intel Security, Palo Alto Networks, and Symantec (all major competing cybersecurity companies) founded the Cyber Threat Alliance in order to "disperse threat intelligence on advanced adversaries across all member organizations to raise the overall situational awareness in order to better protect their organizations and their customers."[61] According to John Davis of Palo Alto Networks, the belief of the group is that threat data should be shared and companies should compete on the implementation of the data.[62] John Lambert of Microsoft claims modern defenders share

information even within lines of competition, based on trusting individuals, and not to support a transactional relationship.[63] The private sector has become a robust and capable group disrupting threats for more than just profit. The unique capabilities of the private sector should be incorporated into national strategy where possible.

Tactical-level Agency Integration and Counter Threat Teams: Agility at the tactical level of cyber operations is vital to an effective cyber strategy able to conduct the full range of counter-threat operations. The tactical level is most often overlooked in organizational discussions in cyberspace, but tactical partnerships provide the most vital quality needed to operate against threats: flexibility. Franklin Kramer claims that the future of cyberspace may vary greatly from today, and cyber strategy must create structures, processes, and people able to adapt to changes in this environment.[64] Kramer's claim that flexibility is needed to operate in a constantly changing environment is accurate, but for more reasons than just the manmade nature of the domain. The policy environment of cyberspace and the threats that operate in the domain have been as dynamic as the domain itself. Nearly all cyber actors currently seem to be significantly concerned with having their actions tied to their organization; many threats will react to an organizational disruption by extensively redesigning their hacking infrastructure to regain anonymity. This redesign may include substantially different areas of grayspace and threat expertise should not be lost due to a different agency becoming operational lead.

Threat-based agencies already have the authorities needed to operate against their respective threats, but those authorities may be limited based on geography or state of conflict. The NSC often looks to build interagency options from the start.[65] Yet many operational solutions presented to the NSC in a stovepiped, agency-specific approach. There are many political factors that may be the reason including funding competition, authority-specific

approval issues, and, especially in cyberspace, there are numerous classification issues. Many cyber capabilities are maintained at an incredibly high, agency-specific classification. The US system of cyber operations is built on extreme anonymity, making it very difficult to cooperate across agencies. The incentives for agency-specific responses must change. A single agency rarely has all the authorities necessary to act at the tactical level across the breadth of adversary infrastructure, and the adversary is aware of this.

Tactical cooperation should occur throughout the spectrum of counter-threat operations. The three parts of this counter-threat cyber strategy should form the platform for tactical groupings of organizations. For example, each sector should have a group to integrate defensive actions with counter-threat operations. For threat pursuit operations, coordination above the tactical level is occurring, sometimes painfully, and is well codified in policy. Below the official coordination level, it is up to agencies to determine how to cooperate at the level where operations actually occur. Senior government leaders must encourage this cooperation and build structures to measure interagency mission accomplishment.

This cyber strategy is a practical look at what defense-in-depth actually means in the interagency cyber policy environment, and why disruption of threats is critical to an effective defensive strategy. A firm understanding of adversary methodology, existing policy and law is sufficient to meet the needs of policy makers without major restructuring. Threat disruption capability should be built in concert with defensive forces for a wide range of threats and any spectrum of conflict. The only way to provide effective cybersecurity is to focus defensive capability on the most critical resources and augment gaps in the system with robust threat pursuit and disruption operations built on existing legal authorities. The methodology to defend the nation from sophisticated cyber adversaries requires a more advanced, efficient, and flexible

strategy that is realistic in the current interagency policy environment and built on knowledge of the threats we face in the cyber domain.

REQUIREMENTS FOR AN EFFECTIVE CYBER STRATEGY

An effective cyber strategy must take into account the dynamics of a complex cyber terrain and threat spectrum, and marry this with the political considerations that accompany operations in the domain. This cannot be ignored or dismissed for strategy to be successful. There is considerable inertia to continue conducting business in the cyber domain the way it has been done for nearly 20 years, but based on the rising threat levels, this is not an effective strategy. There are two schools of thought regarding cyberspace operations policy. The first is to grant more extensive or intrusive authorities to agencies so they can fight more effectively in their own autonomous stovepipes, and the second is to work within the system and implement a strategy that takes existing policy and authorities into account. This strategy proposes a cooperative solution that builds capabilities at all levels to operate within the political considerations of the interagency.

Necessary Qualities of Cyber Strategy

- Be Flexible across Threats and Spectrum of Conflict
- Prioritize Threats, Missions, Information/Technology, and Capabilities
- Ensure Readiness

Political Considerations

- Cooperate with Allies
- Demonstrate Restraint, Manage Escalation
- Create Norms to Reduce Threat Ambiguity, Ensure Intent is More Easily Inferred
- Deny Safe Haven
- Create the Least Amount of Change to Existing Policy and the Interagency Process

Be Flexible across Threats and the Spectrum of Conflict: The first quality needed to implement an effective cyber strategy is flexibility. There are two factors that require flexibility for cyber organization: 1) diversity of cyber threats, and 2) the state of conflict. All parts of the Executive Branch with a mission to disrupt threats already possess the needed authorities to execute their missions, but how, when, and where agencies operate may require slight reorganization of command and control relationships in cyber teams. Some of the basic assumptions may be invalid, and this is where friction occurs. Through understanding the political considerations, this friction can be avoided and operations can achieve measurable effects. Some existing concepts about when and where to employ forces and the command and control relationships at the tactical level may not be appropriate for the cyber domain in order to provide operational flexibility.

The complexity of the threat spectrum impacts flexibility, and political leaders prefer to use the most appropriate authority for each part of the threat spectrum. There is a notable difference between authority and agency; these are not synonymous terms. For instance, counterintelligence authority is most closely associated with countering nation-state intelligence threats. Especially during peacetime, counterintelligence is not a geographically limited authority as long as coordination mechanisms are exercised during operational activity.[66] Counterintelligence is often fused closely with law enforcement authority and is the most preferred authority for operations conducted within the United States.[67] Foreign intelligence authority resides within the different parts of the US intelligence Community (IC) and is heavily restricted domestically. The IC looks across foreign threats and provides information to decision makers about the full spectrum of threats overseas. From a standpoint of disrupting threats, the IC is primarily oriented around gathering information to support targeting for action based

authorities or crafting policy responses. Cyberspace brings those threats into the nation. The IC alone does not have the flexibility to act to disrupt threats in cyberspace throughout hacking infrastructure, but when fused with agencies with domestic authority, this can be highly effective at disrupting threats while maintaining privacy concerns.

Prioritize Threats, Missions, Information/Technology, and Capabilities: Cyberspace has allowed threats to move beyond their borders and interact with US targets. Defense is not hopeless, but it needs to be done more efficiently. We need a new model for the Chief Information Officer responsible for building the enterprise capability of their organization. Before designing cybersecurity measures in an organization, the following criteria should be evaluated:

1. What are the critical missions?
2. What information or technology is most essential to the core missions?
3. What capabilities/operations does the organization need to ensure?
4. What threats are most likely to target these missions, information/technology, or capabilities?

This assessment is done at all levels. It provides a baseline for how robust the defenses are needed for an organization and where. Once this is determined, each sector assesses which threats are most important to track and disrupt. After this is accomplished, an interagency task force prioritizes threat pursuit operations based on the mission priority to the government and agencies responsible for tracking and disrupting threats in cyberspace.

Ensure Readiness: The spectrum of conflict will dictate when some agencies are able to act, but readiness for conflict in cyberspace is essential. The military, often referred to as Title 10 forces, is the part of the government built for contingency operations. The military is used to address a wide variety of threats and its fundamental charter remains unchanged in cyberspace. Military cyber forces must be ready to act in times of crisis. The military must be able to

manipulate the cyber environment, but should avoid direct use of force against threats except when warranted due to the spectrum of conflict. The DoD Cyber Strategy states, "As a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the US Homeland or US interests before conducting cyberspace operations."[68] The military must still ensure readiness for conflict by gaining threat expertise and building capabilities necessary to defeat cyber threats that can be implemented quickly. The complication for military readiness occurs in times of peace based on the political realities of hacking infrastructure in grayspace. Military authority is purpose built for significant threats, but US policy chooses to exercise military use of force with restraint.

There are three proposed phases of operations in cyberspace: steady state, shaping, and contingency.[69] Steady state operations focus on maintaining a manageable threat level. Cyberspace is a continually evolving domain, and nations throughout the world can join in cyber espionage or cyberwarfare with a low barrier to entry, and realistic cyber strategy does not assume that these threats can be altogether eliminated. Nation-state cyber threats are bound to the foreign policy of their nations. Steady state operations should focus on building cooperation in cyberspace, establishing norms, and working towards ways to ensure conflict in the domain or elsewhere is avoided. Continually improving cyber defenses and thinking about how critical missions touch the cyber domain are also essential elements. Information sharing should become the norm. As the private sector has demonstrated, they are willing to work together to stop threats from exploiting victims, and the government should support those actions however possible. Shaping operations are designed to maneuver the adversary into areas of greater advantage for the United States. Threats in the cyber domain all inherently deceive the networks they are trying to penetrate by impersonating legitimate users.[70] Shaping operations manipulate

these adversaries at the points of greatest advantage, by turning the deception in favor of the defender. This includes actions designed to disrupt their hacking activities either through operational action, diplomacy, sanctions, or other instruments of power. Shaping operations are needed to contain and manage threats that are reaching unacceptable levels. Contingency operations are capabilities that will be needed if threats shift the threat spectrum to cause significant harm to the US, its allies, or its interests. Contingency capabilities are critical for the US military. It includes being prepared to defend against an advanced threat with a foothold in our networks. We must be able to disrupt threats in the most extreme situations through capabilities that use force when necessary through the cyber domain. The military must also have the capability to hold targets at risk should the need arise. Regardless of the spectrum of conflict, the United States must be ready to operate to stop cyberspace threats

Political Considerations: Strategy is a part of the political structure of the nation and must be subordinate to the will of the nation and political leadership. Even if a solution may be ideal for handling a threat, it may sacrifice too much in other political areas to be viable. Managing political considerations are essential for strategy to be effective, and ignoring these will lead to failure. Operations in cyberspace will always be subordinate to foreign policy and cyber strategy will always be subordinate to the greater US National Security Strategy. Operations should consider that actions in cyberspace may have consequences in other domains, or for diplomacy. The list of considerations are based on commonly seen situations and will guide organizations in the implementation of cyber strategy. They are not intended to be all inclusive, and strategy will always evolve as the threat landscape and the cyber domain evolve.

Cooperate with Allies: In national strategy, the United States has demonstrated a strong desire to cooperate as broadly as possible in cyberspace. By joining with allies to defend against

threats, actions in cyberspace gain legitimacy. Many allies have robust capabilities to track adversary infrastructure within their own borders or abroad. This principle is clearly articulated in the Cybersecurity National Action Plan (CNAP).

> Better securing our own digital infrastructure is only part of the solution. We must lead the international effort in adopting principles of responsible state behavior, even while we take steps to deter and disrupt malicious activity. We cannot pursue these goals alone – we must pursue them in concert with our allies and partners around the world.[71]

The intent of the CNAP here appears to extend beyond just cybersecurity to a principle of disrupting threats, a critical component of this cyber strategy. America acts alone only when necessary. Fostering strong operational relationships with allies is essential to deny safe havens for hacking infrastructure. In an ideal world, every nation would be responsible for disrupting hacking infrastructure within their borders and would cooperate to quickly act when needed to stop cyber attacks. Even in the United States, this is not realized, but all nations should strive toward this goal and work together to build capability to disrupt advanced cyber threats.

Demonstrate Restrain and Manage Escalation: Not all threats in cyberspace require an aggressive response to disrupt them. Furthermore, every operational action carries with it consequences for foreign policy. The complexity nations face initially determining attribution of cyberspace activity may have led to the perception that actions can be taken in cyberspace without consideration to escalation, and this is not the case. In some cases, action in cyberspace may not be the preferred option to manage escalation. In foreign policy, the most escalatory option is often military action, but the military necessarily has the most capacity to conduct cyber operations. Outside the cyber domain, combat forces are not used when an espionage threat is detected. Although there is no international agreement authorizing a nation to conduct espionage activity against another, all nations do it. Traditionally, counterintelligence forces (including within the military) are used to identify, track, and disrupt espionage threats. Like Title 10

military forces, counterintelligence can act to disrupt threats, but is more appropriately used in peacetime to disrupt adversary espionage activity.

The implications for the military use of cyberspace are even more problematic. To effectively operate in cyberspace in an era of austerity, we need to rethink the way we use cyberspace for military operations and devise a military strategy that can function in the modern interagency policy environment instead of ignoring the implications of the use of military force in peacetime against nations that we are intrinsically linked through other aspects of US foreign policy. Secrecy and cyber-enabled anonymity does not alleviate the need for military restrain. The military should be ready to act to stop advanced threats, but military options should be used only carefully to avoid escalation.

Create Norms to Reduce Threat Ambiguity, Ensure Intent is More Easily Inferred: The US should seek to reduce threat ambiguity in cyberspace. One of the large problems in responding to cyber threats is the complexity from the way threats operate to anonymize their activity that makes it very difficult to determine intent. For example, Chinese state sponsored espionage groups have conducted theft of intellectual property in order to provide competitive advantage to Chinese corporations. The problem with this activity is the United States considers this type of activity criminal in nature as evidenced by the indictments against Chinese espionage actors. Recently, the US and China agreed to discontinue this type of espionage activity.

> "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[72]

The blending of criminal and espionage activity can go the other direction as well. Russia is widely believed to use criminal hacker organizations to support national security objectives.[73] The linkages between crime and espionage are significant, but the greatest concern from a

national security context may be the blending of cyber infrastructure between nation-state intelligence and militaries. Many significant cyber espionage threats have blended their espionage infrastructure and/or organizations with their offensive military capabilities. This ambiguity means if hostile activity is detected in a sector like nuclear power, it may be extremely difficult to determine intent at the early stage of an incident such as the one below:

> "South Korean investigators said state-owned Korea Hydro, which operates the country's 23 nuclear reactors, and its business partners were targeted in multiple cyberattacks aimed at stealing internal data that included plant blueprints and employees' personal information."[74]

This same incident could have been interpreted as espionage, criminal intellectual property theft, or a prelude to a use of force against the plant. Misperceptions about an incident such as this one could quickly escalate tensions if intent in cyberspace cannot be easily determined. It appears the intent of this North Korean activity was espionage, but the same group was allegedly responsible for destructive action against Sony as well. Although this did not occur, if a nation like South Korea believes that the penetration they detected was intended to damage a nuclear reactor, they may consider this penetration an extremely dangerous event and overreact. Cyber operational methodology should attempt to reduce this ambiguity wherever possible.

Deny Safe Haven: There is far too much territory in cyberspace that is effectively ungoverned from a standpoint of managing cyber threats. This is not meant to imply that the servers physically reside in areas without governments. A safe haven in cyberspace is an area in foreign policy or domestic law where an actor can exploit the freedom to act without the ability for nations to effectively disrupt threats at this location. This can occur in the United States as easily as in a foreign nation like Belarus. There are numerous ways to deny safe havens for hostile cyber actors. The Budapest Convention on Cybercrime is an example of diplomatic efforts to agree on norms to act within sovereign areas against cyber threats.[75] Another example

would be to block internet traffic from an area that a threat has learned to exploit. This could be done at a victim or at a Tier 1 Internet Service Provider depending on the scope of the problem. Domestic law may provide a safe haven in some areas if implemented poorly. Privacy must always be balanced with the need to act against threats, and nothing in this strategy is meant to reduce privacy, but structures are needed to act quickly if probable cause is found. Processes that take months or longer are not sufficient to disrupt threats. It is important to preserve the rights of citizens while denying threats the ability to create hacking infrastructure outside the reach of effective governance.

Create the Least Amount of Change to Existing Policy and the Interagency Process: There have been many discussions at high levels of the government that the reason we as a nation have struggled with cybersecurity have been because our laws and policies are outdated.

> WASHINGTON — The Army intelligence officer nominated to lead the Pentagon's new command devoted to warfare in cyberspace has warned Congress that policy directives and legal controls over digital combat are outdated and have failed to keep pace with the military's technical capabilities.
> The officer, Lt. Gen. Keith B. Alexander, wrote to members of the Senate Armed Services Committee that computer network warfare was evolving so rapidly that there was a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."[76]

There is certainly room to improve the speed and efficiency of the interagency approval processes, but the problem is usually not the law or policies. Between all the authorities of the federal government and the private sector, effective cybersecurity is possible, but we have to ask ourselves if we are organized correctly to disrupt threats in the cyber domain. The complexities of the cyber domain have led to an inability to work in stovepipes and be effective, and that may not a comfortable position for the United States Government. There will rarely, if ever, be an effective plan by a single agency to defeat a cyber threat. We are going to have to work together and we are going to have to give up some agency control to lead against different threats in

appropriate phases of conflict. Options to disrupt threats should be built as interagency from the start. In other domains, organizations were possibly built with all the tools needed to operate against a threat, but in cyberspace threats exploit the friction of interagency politics. It is not necessary to rewrite authorities in order to act in cyberspace. At different phases or parts of operations, the appropriate agency will execute their approval process. In many cases, a unique authority like counterintelligence may be the most ideally suited to disrupt a threat activity in peacetime, but as a threat evolves, this may need to transition to military authority. The same could be true of US foreign intelligence identifying the locations and key points to disrupt a threat for another agency to act upon.

Executing Effective Strategy in Cyberspace: Cyberspace is a unique and complicated domain from a standpoint of policy, but cyberspace strategy need not lead us to the idea we must defend the totality of cyberspace against the most advanced threats. Cybersecurity is a complicated term, but it should mean far more than just better defensive perimeters and practices. To truly be effective in turning the tide in cyberspace we must take threats into account. This cyber strategy factors in how threats operate and the tools the nation uses to disrupt threats. A flexible interagency strategy is needed to ensure we are ready to frustrate and defeat threats and ensure the US does not suffer significant consequences in cyber domain.

---

[1] Sun Tzu, *The Art of War*, translated by Lionel Giles, 1910, http://suntzusaid.com (accessed 23 July 2015), Ch 6.
[2] Cybersecurity Ventures "Cybersecurity Market Report," http://cybersecurityventures.com/cybersecurity-market-report-q2-2015/ (accessed 25 Mar 2016).
[3] Sebastian Convertino, Lou Anne DeMettei, and Tammy Knierim, *Flying and Fighting in Cyberspace, Air War College Maxwell Paper No. 40*, (Maxwell AFB, AL: Air University Press, July 2007). Iv.
[4] Interview with John Davis, Washington, DC: 14 Mar, 2016.
[5] Infosec Institute, "Hacktivism: Means and Motivations … What Else?" 2 October 2013. http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/ (accessed 25 Mar 2016)
[6] Ibid.
[7] New York Times, "Anonymous (Internet Group)" http://www.nytimes.com/topic/organization/anonymous-internet-group (accessed 26 Mar 2016).

[8] Radio Free Europe, "What Is 'Anonymous' And How Does It Operate?" 29 February 2012. http://www.rferl.org/content/explainer_what_is_anonymous_and_how_does_it_operate/24500381.html (accessed 26 March 2016).
[9] Center for Strategic and International Studies, *The Economic Impact of Cybercrime and Cyber Espionage* (July 2013).
[10] Council of Europe, "Full List: Convention on Cybercrime, Budapest" http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed 30 March 2016).
[11] The Federal Bureau of Investigation, "Identity Theft," https://www.fbi.gov/about-us/investigate/cyber/identity_theft)accessed 30 March 2016).
[12] Paul Reynolds, "The world's second oldest profession," (BBC News Online, 26 February 2004) http://news.bbc.co.uk/2/hi/americas/3490120.stm (accessed 30 March 2016).
[13] "Rehab and the Spies" https://www.biblegateway.com/passage/?search=Joshua+2&version=NIV (accessed 20 May 2016).
[14] Martin Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: Rand Corporation, 2012), xviii.
[15] Ibid., xi.
[16] Charles J. Dunlap Jr., "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos et al. (Boca Raton, FL: Taylor & Francis Group, 2014), 215.
[17] Ray Sanchez, "ISIS exploits social media to make inroads in U.S." (CNN, 5 June 2015) http://www.cnn.com/2015/06/04/us/isis-social-media-recruits/ (accessed 30 March, 2016).
[18] Michael Hayden, "The Future of Things Cyber," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos et al. (Boca Raton, FL: Taylor & Francis Group, 2014), 5.
[19] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA).
[20] David Kushner, "The Real Story of Stuxnet" (IEEE Spectrum, 26 Feb 2013) http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed 13 Apr 2016)
[21] Dictionary.com "Infrastructure" http://www.dictionary.com/browse/infrastructure
[22] Mandiant, *APT1*, 41-44.
[23] Mandiant, *APT1,* 39.
[24] Michael Hayden, "The Future of Things Cyber," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos et al. (Boca Raton, FL: Taylor & Francis Group, 2014), 3.
[25] The White House, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003).
[26] Interview with Fortune 50 cybersecurity expert, Washington DC, 13 Mar 2016.
[27] Jason M. Breslow, "With or Without the Patriot Act, Here's How the NSA Can Still Spy on Americans," (PBS.org: 1 Jun, 2015) http://www.pbs.org/wgbh/frontline/article/with-or-without-the-patriot-act-heres-how-the-nsa-can-still-spy-on-americans/ (accessed 17 Apr 2016).
[28] Spencer Ackerman and Sabrina Siddiqui, "NSA surveillance opposed by American voters from all parties, poll finds" (The Guardian, 18 May 2015) http://www.theguardian.com/us-news/2015/may/18/us-voters-broadly-opposed-nsa-surveillance (accessed 17 Apr 2016).
[29] Andy Greenberg, "How Hackers Hid a Money Mining Botnet in the Clouds of Amazon and Others" (Wired.com: 24 Jul 2014) http://www.wired.com/2014/07/how-hackers-hid-a-money-mining-botnet-in-amazons-cloud/ (accessed 21 Apr 2016).
[30] Cyber Threat Alliance, "Cyber Threat Alliance," http://cyberthreatalliance.org/mission.html (accessed 18 Apr 2016).
[31] This is common in many terms of service for almost all major cloud providers. Major corporate service providers are not leasing space on the Internet in order to facilitate illegal activity. The Amazon Web Services Terms of Service is provided as an example: Amazon Web Services, "AWS Service Terms" (Amazon.com: 19 Apr 2016) https://aws.amazon.com/service-terms/ (accessed 21 Apr 2016).
[32] US Archives, "Constitution of the United States," http://www.archives.gov/exhibits/charters/constitution_transcript.html (accessed 21 Apr 2016).

[33] The White House, *Executive Order 12333--United States intelligence activities* (Washington, DC: National Archives, 1981) http://www.archives.gov/federal-register/codification/executive-order/12333.html (accessed 23 July 2015).
[34] US Department of Justice, Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage" (19 May 2014) https://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage (accessed 17 Apr 16).
[35] US Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, "Electronic Communications Privacy Act of 1986 (ECPA) 18 USC 2510-22" https://it.ojp.gov/privacyliberty/authorities/statutes/1285.
[36] Gen. Stephen R. Lorenz, Air Education and Training Command commander, "Lorenz on Leadership: At War in Cyberspace," (Randolph AFB, TX: 9 Jan 2009).
[37] "10 U.S. Code § 130g - Authorities concerning military cyber operations," https://www.law.cornell.edu/uscode/text/10/130g.
[38] "50 U.S. Code § 3093 - Presidential approval and reporting of covert actions" https://www.law.cornell.edu/uscode/text/50/3093 (accessed 19 Apr 2016).
[39] Associated Press, "Defense Department launches cyberwar against ISIS" (New York Post: 26 Feb 2016) http://nypost.com/2016/02/26/defense-department-launches-cyberwar-against-isis/ (accessed 20 May 2016).
[40] Charles Dunlap Jr., "Cyber Strategists on Cyberlaw for Cyberwar," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos et al. (Boca Raton, FL: Taylor & Francis Group, 2014), 214-215.
[41] Frederick the Great, http://www.brainyquote.com/quotes/quotes/f/frederickt140989.html (accessed 23 July 2015).
[42] Internet Live Stats, "Internet Users in the World" http://www.internetlivestats.com/internet-users/ (live stats, accessed 18 Apr 2016).
[43] This quote is a famous Churchill quote. This article on the Internet was about defense spending that used the quote as a title: Lawrence Ferrell, Jr. "Gentlemen, We Have Run Out Of Money; Now We Have to Think" (National Defense Magazine: Nov 2011) http://www.nationaldefensemagazine.org/archive/2011/November/Pages/%E2%80%98Gentlemen,WeHaveRunOutOfMoney;NowWeHavetoThink%E2%80%99.aspx (accessed 21 Apr 2016)
[44] "75 billion devices will be connected to the internet by 2020," http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10 (accessed 21 Apr 2016).
[45] The White House, "FACT SHEET: Cybersecurity National Action Plan," https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (accessed 18 Apr 2016).
[46] Ibid.
[47] Interview with John Davis, Washington, DC: 14 Mar, 2016.
[48] Michael Hayden, "The Future of Things Cyber," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos et al. (Boca Raton, FL: Taylor & Francis Group, 2014), 8.
[49] John Lambert at Kaspersky Security Analyst Summit, 25 Feb 2016. https://www.youtube.com/watch?v=Ig2bbfSzBCM (accessed 18 Apr 2016).
[50] Trend Micro, "SIMBA: A Botnet Takedown," (12 Apr 2015) http://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/ (accessed 18 Apr 2016).
[51] Shannon Tiezzi, "China's Response to the US Cyber Espionage Charges: China is furious over charges brought against 5 PLA officers – and things could get worse before they get better," (The Diplomat, 21 May 2014) http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/ (accessed 18 Apr 2016).
[52] Zoe Li, CNN, "What we know about the Chinese army's alleged cyber spying unit" (CNN, 20 May 2014) http://www.cnn.com/2014/05/20/world/asia/china-unit-61398/ (accessed 18 Apr 2016).
[53] EO12333, DoDI 5240.1-R, Foreign Intelligence Surveillance Act, and the Electronic Communications Privacy Act provide procedures for counterintelligence operations overseas and in the United States. Some agencies are restricted from conducting missions within the United States.
[54] Mandiant, *APT1*, 24.
[55] Interview with a source familiar with the NSC process, Washington DC, 14 Mar 2016.

[56] The White House, "FACT SHEET: Cyber Threat Intelligence Integration Center," (25 Feb 2015) https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center (accessed 18 Apr 2016).
[57] The Federal Bureau of Investigation, "National Cyber Investigative Joint Task Force," https://www.fbi.gov/about-us/investigate/cyber/ncijtf (accessed 18 Apr 2016).
[58] Mandiant, *APT1*.
[59] Crowdstrike Global Intelligence Team, *Crowdstrike Intelligence Report: Putter Panda*. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi548eTwOnMAhVE7YMKHUsGAmMQFggcMAA&url=https%3A%2F%2Fcdn0.vox-cdn.com%2Fassets%2F4589853%2Fcrowdstrike-intelligence-report-putter-panda.original.pdf&usg=AFQjCNGMPNsmSAt1X_O7KdTzeJN2QPlOmA&sig2=_-xj9iPQ2GUtvcRzqD7cJg&bvm=bv.122676328,bs.2,d.dmo (accessed 20 May 2016).
[60] Interview with Fortune 50 cybersecurity expert, Washington DC, 13 Mar 2016.
[61] Cyber Threat Alliance, "Cyber Threat Alliance," http://cyberthreatalliance.org/mission.html (accessed 18 Apr 2016).
[62] John Davis speaking at Cyber 912 Competition, Washington, DC: 12 Mar 2016.
[63] John Lambert at Kaspersky Security Analyst Summit, 25 Feb 2016. https://www.youtube.com/watch?v=Ig2bbfSzBCM (accessed 18 Apr 2016).
[64] Franklin Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security,* ed. Franklin Kramer, Stuart Starr, and Larry Wentz et al. (Washington, DC: Potomac Books, 2009).
[65] Interview with a source familiar with the NSC process, Washington, DC: 14 Mar 2016.
[66] EO12333, DoDI 5240.1-R, Foreign Intelligence Surveillance Act, Electronic Communications Privacy Act provide procedures for counterintelligence operations overseas and in the United States. Some agencies are restricted from conducting missions within the United States.
[67] EO12333, DoDI 5240.1-R, Foreign Intelligence Surveillance Act, Electronic Communications Privacy Act.
[68] The Department of Defense, *The DoD Cyber* Strategy (Washington, DC: April, 2015), 5.
[69] This concept was based on a conversation with a source familiar with the National Security Council.
[70] This is based on a conversation with Lt Col David Vernal, USAF.
[71] The White House, "FACT SHEET: Cybersecurity National Action Plan," https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (accessed 18 Apr 2016).
[72] The White House, "FACT SHEET: President Xi Jinping's State Visit to the United States" (25 Sep 2015) https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed online 20 Apr 2016).
[73] Brian Whitmore, Radio Free Europe/Radio Liberty, "Organized crime is now a major element of Russia statecraft," (Business Insider: 27 Oct 2015) http://www.businessinsider.com/organized-crime-is-now-a-major-element-of-russia-statecraft-2015-10 (accessed 20 Apr 2016).
[74] Jeyup S. Kwaak, "North Korea Blamed for Nuclear-Power Plant Hack," (The Wall Street Journal: 17 Mar 2015) http://www.wsj.com/articles/north-korea-blamed-for-nuclear-power-plant-hack-1426589324 (accessed 20 Apr 2016).
[75] Council of Europe, "Details of Treaty #185," (07 Jan 2004) http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (accessed 20 Apr 2016).
[76] Thom Shanker, "Cyberwar Nominee Sees Gaps in Law" (The New York Times: 14 Apr 2010) http://www.nytimes.com/2010/04/15/world/15military.html?_r=0 (accessed 20 Apr 2016).